TCESP
Tribunal de Contas
do Estado de São Paulo

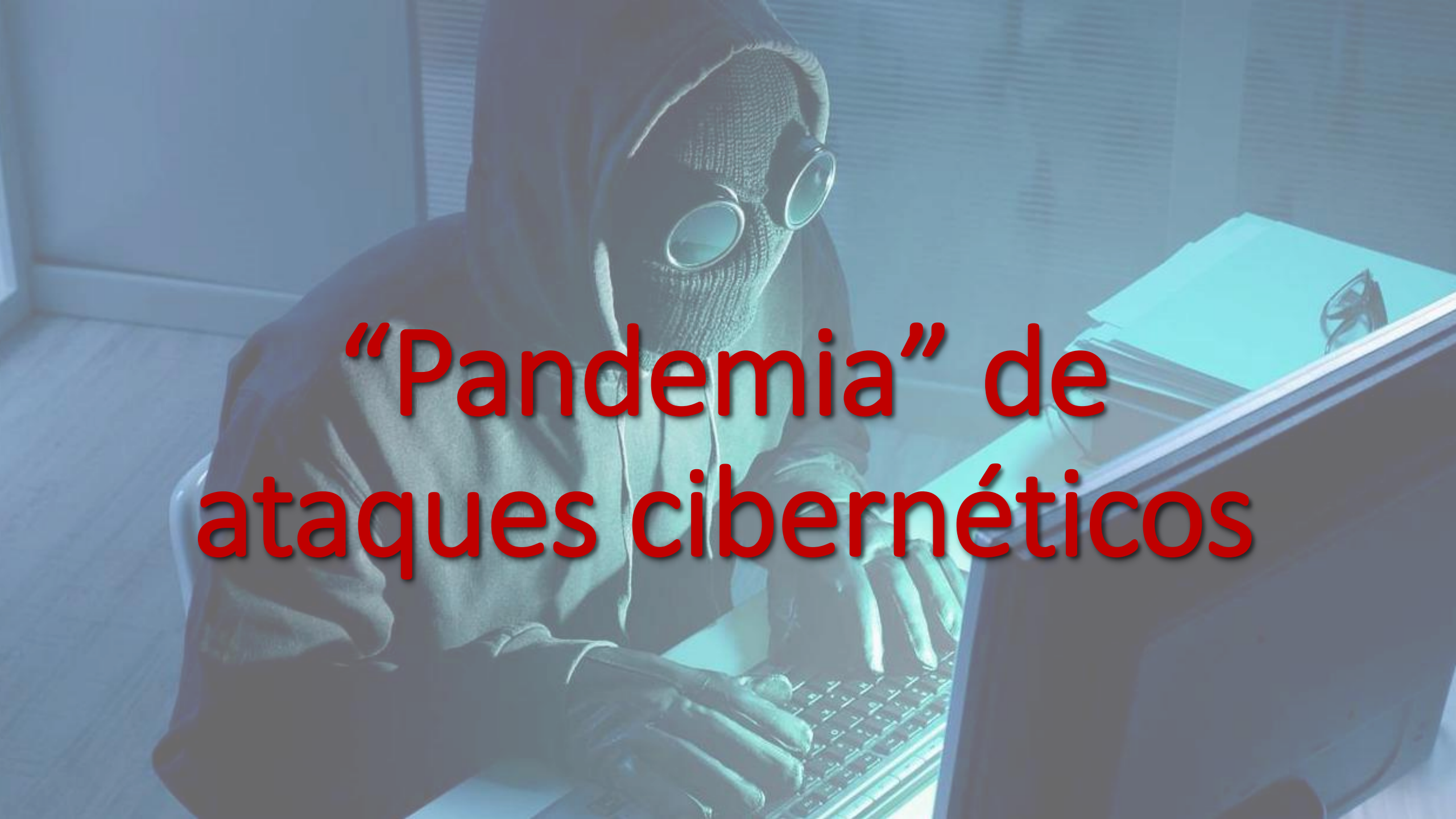
Passos mínimos para adequação à LGPD

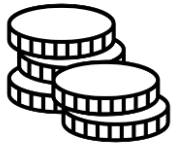
Fabio Correa Xavier

Diretor do Departamento de Tecnologia da Informação

Tribunal de Contas do Estado de São Paulo

DTI.TCESP


“Pandemia” de
ataques cibernéticos



Em 2021

US$ 6 trilhões

prejuízo global

https://bit.ly/3ucPkSf

Prejuízo global com ataques cibernéticos a empresas deve chegar a US$ 6 trilhões em 2021

Maria Amélia Ávila
mvarginha@hojeemdia.com.br

24/09/2021 - 07h00

Compartilhe Link: http://hoje.vc/3b810

O prejuízo das empresas em todo mundo com crimes cibernéticos em 2021 deve ser três vezes o valor do Produto Interno Bruto (PIB) brasileiro - US$ 6 trilhões. O Brasil ocupa o 5º lugar com mais registros de ataques hackers contra empresas. Só neste ano, foram registradas 9,1 milhões de ocorrências, deixando o país atrás apenas de EUA, Reino Unido, Alemanha e África do Sul. Os dados são da empresa de consultoria alemã Roland Berger.

TCESP
Tribunal de Contas
do Estado de São Paulo

35,3%
Governo

9,7%
Indústria

9,2%
Saúde

Governo é o principal alvo de ataques cibernéticos no Brasil, revela análise

Por Felipe Gugelmin | Editado por Claudio Yuge | 06 de Julho de 2021 às 11h20

Com a pandemia e o isolamento social decorrente dela, muitas pessoas intensificaram seu uso da internet e dos meios digitais. A tendência também foi seguida pelos criminosos, que intensificaram suas atividades para aproveitar as vulnerabilidades geradas pelo trabalho remoto e por campanhas como a do Auxílio Emergencial, no caso brasileiro.

- Aumentam os ataques de ransomware a sistemas industriais desatualizados
- EUA e Reino Unido acusam Rússia de ciberataques a infraestruturas de nuvem
- Conhecimento público geral sobre ciberataques ainda é baixo, confirma pesquisa

Segundo um estudo conduzido pela Trend Micro, a maioria dos ataques no Brasil se concentrou em prejudicar entidades ligadas ao governo (35,3%). Em seguida, os principais alvos foram o setor da manufatura (9,7%) e da saúde (9,2%) em uma tendência que destoou um pouco dos números globais.

https://bit.ly/3ERfi2L

TCESP
Tribunal de Contas
do Estado de São Paulo

Quanto custa um incidente de segurança?

TCESP
Tribunal de Contas
do Estado de São Paulo

Custo médio por país

US$ 3,86 milhões
Média mundial por incidente

US$ 8,64 milhões
USA

US$ 1,12 milhões
Brasil

Custo médio por setor

US$ 7,13 milhões
Saúde

US$ 6,39 milhões
Energia

US$ 5,85 milhões
Financeiro

US$ 1,08 milhões
Governo

Tempo médio para identificar e mitigar incidentes

280 dias

207 identificar
73 mitigar

380 dias

Pior média mundial

329 dias

Saúde tem a pior média

US$150
cada dado pessoal

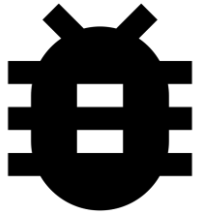
LGPD
Lei 13.709/18

80%
incidentes
com dados pessoais

Causas dos incidentes

Ataques Maliciosos

52% no geral
47% no Brasil



Falhas de Sistemas

25% no geral
28% no Brasil

Erro Humano

23% no geral
25% no Brasil

Fonte: *Cost of a Data Breach Report* 2020, Ponemon Institute
https://bit.ly/39ErsOc

TCESP
Tribunal de Contas
do Estado de São Paulo

+24%

de 2014 para 2020

Fonte: Ponemon Institute

154,4

milhões de ataques

jan-abr 2021

+90%

em relação jan-abr 2020

Fonte: SonicWall

Principais vetores de *Ransomware*

E-mail *phishing*

E-mails falsos com o objetivo de roubar credenciais

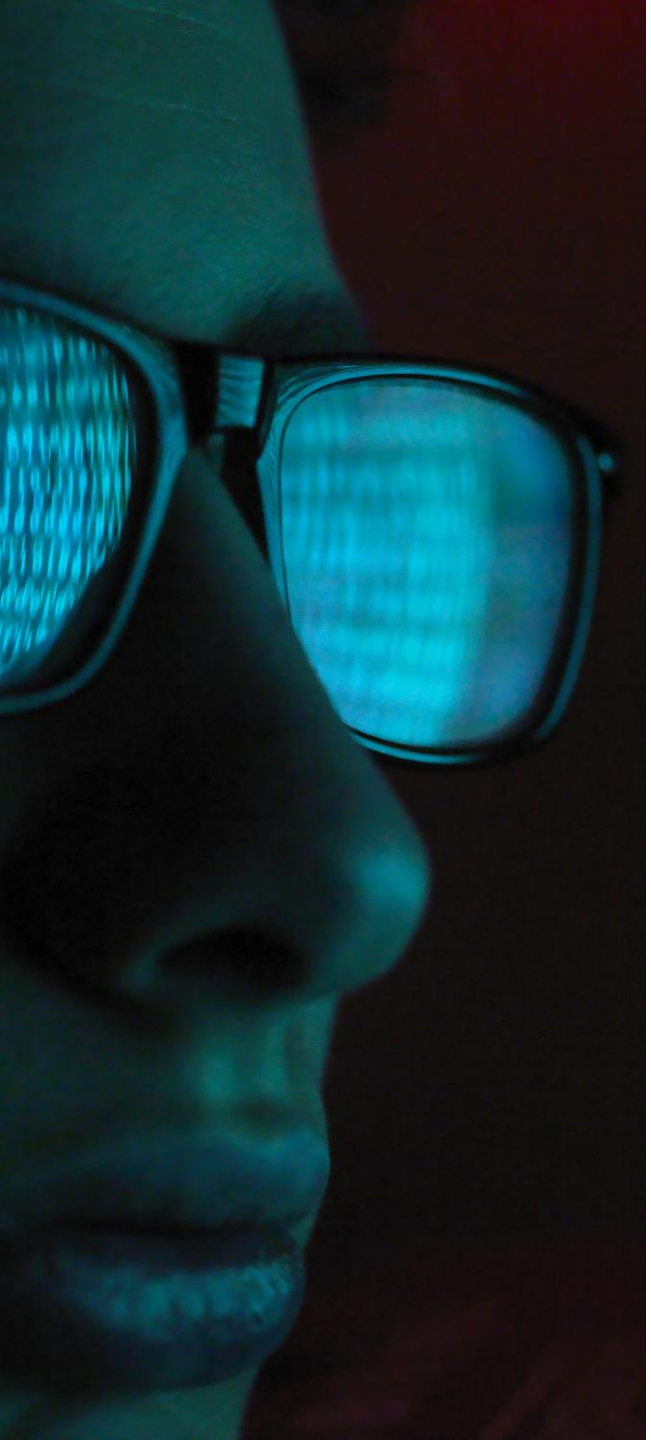
Protocolo RDP

Protocolo Remote Desktop (RDP) é aquele que permite o acesso remoto a computadores por meio da Internet e que ficou muito comum em tempos de pandemia

Vulnerabilidades de softwares

Especialmente de sistemas operacionais, que permitem acesso ao computador da vítima para espalhar o *ransomware*.

Fonte: *o IC3[10] (Internet Crime Complaint Center), ligado ao FBI, em meu artigo "***Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0



Por que somos tão vulneráveis?

TCESP Tribunal de Contas do Estado de São Paulo

1. **Isso não acontece comigo!**
2. **Negligência!!**
   "Esse pessoal de segurança da informação é chato! "
3. **Não aplicar proteções básicas!**
4. **Engenharia Social**
5. **Vulnerabilidade de softwares**

TCESP
Tribunal de Contas
do Estado de São Paulo

E a LGPD?

TCESP Tribunal de Contas do Estado de São Paulo

Multas aplicadas pelas Autoridades europeias (euros)

272,5 milhões
Total

50 milhões
Google

35,26 milhões
H&M

27,8 milhões
TIM

Principais falhas que geraram multas

1. Violação ao princípio da transparência
2. Violação na demonstração da Base Legal que fundamenta o tratamento de dados pessoais
3. Violação na implementação de medidas de segurança apropriadas
4. Violação nos princípios de minimização de dados e limitação de armazenamento

Fonte: Relatório "2021 DLA Piper GDPR fines and data breach notifications", disponível em https://www.gamingtechlaw.com/2021/01/2021-dla-piper-gdpr-fines-data-breach-

TCESP
Tribunal de Contas
do Estado de São Paulo

Notificações

+19%
De 2019 para 2020

278
Por dia,
em 2019

➡

331
Por dia,
em 2020

+281 mil
Desde maio de 2018

Países que mais notificaram

77.747
Alemanha

66.527
Holanda

30.536
Reino Unido

Fonte: Relatório "2021 DLA Piper GDPR fines and data breach notifications", disponível em https://www.gamingtechlaw.com/2021/01/2021-dla-piper-gdpr-fines-data-breach-

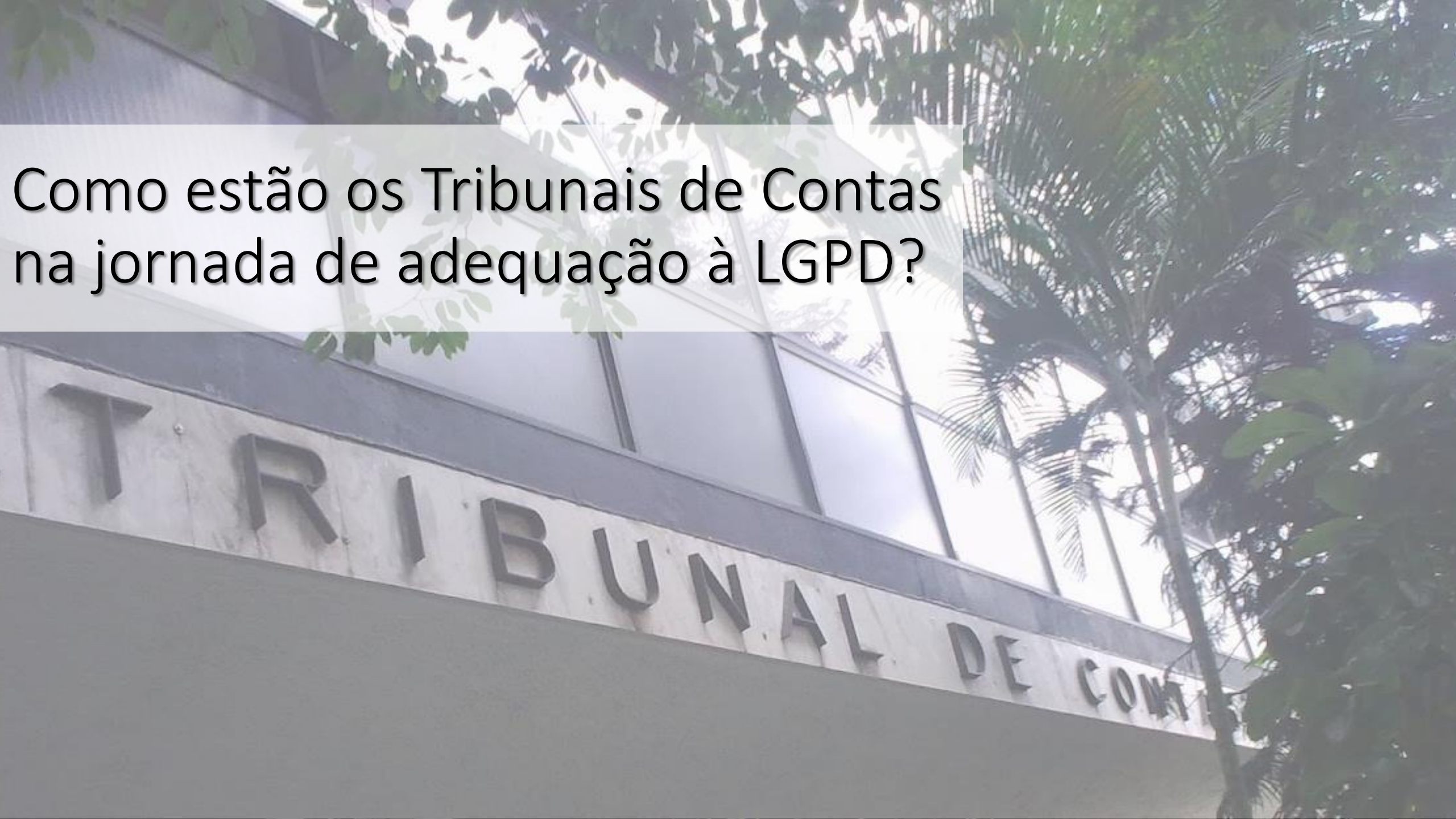
“o poder dessas autoridades de regulação tem sido duramente testado, especialmente no último ano, pois não foram poucos os casos de redução do valor das multas em processos de apelação judicial.

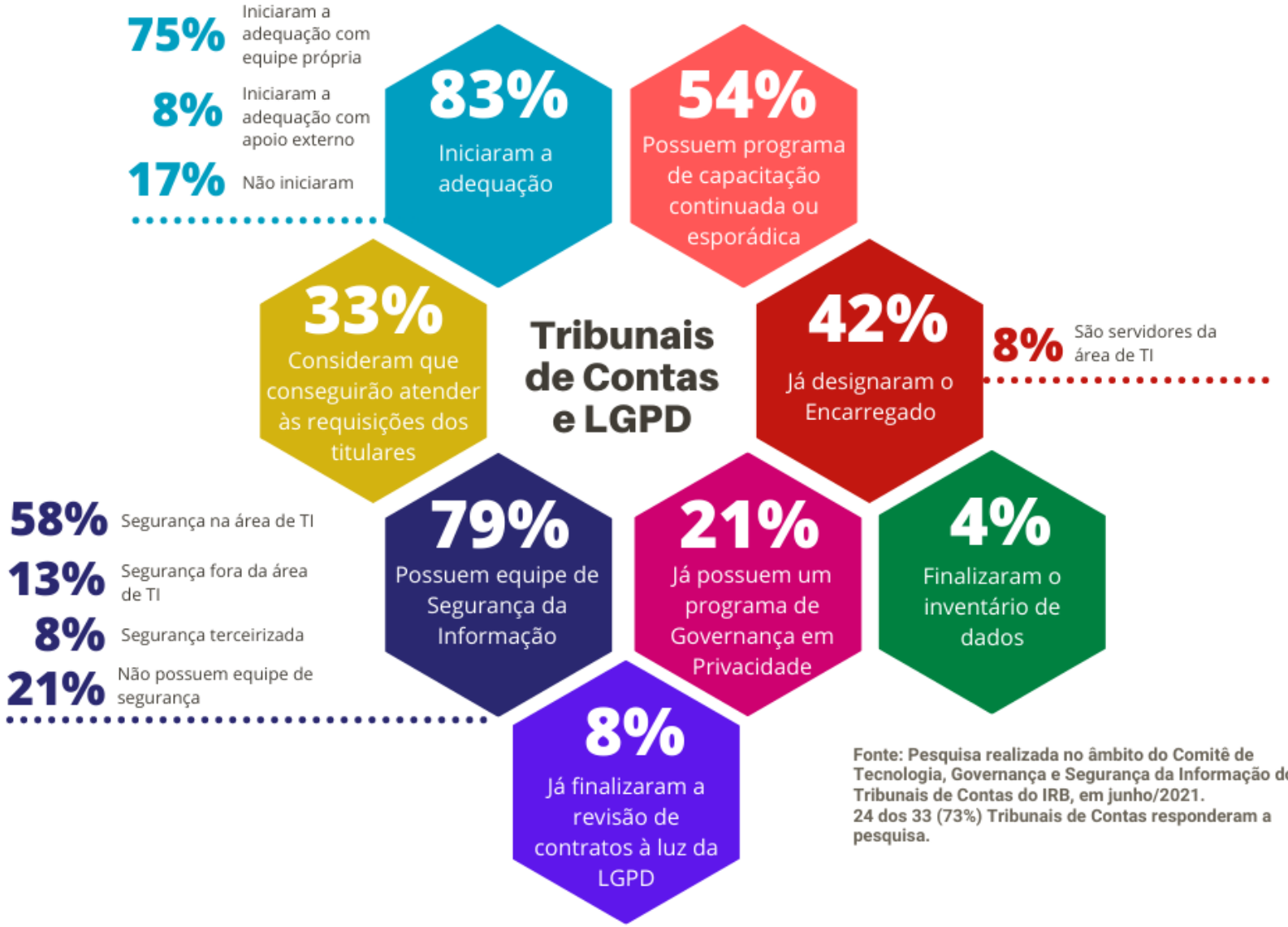
A tendência é que os recursos e defesas fiquem cada vez mais robustos e substanciais.”

Ewa Kurowska-Tober

Copresidente do Grupo de Proteção e Segurança de Dados da DLA Piper

Como estão os Tribunais de Contas na jornada de adequação à LGPD?





Fonte: Pesquisa realizada no âmbito do Comitê de Tecnologia, Governança e Segurança da Informação dos Tribunais de Contas do IRB, em junho/2021.
24 dos 33 (73%) Tribunais de Contas responderam a pesquisa.

Ações mínimas para adequação à

L G P D

Lei nº 13.709/18

01 PROGRAMA DE GOVERNANÇA DE PRIVACIDADE

Conforme art. 50

02 DEFINIÇÃO DO ENCARREGADO DE DADOS

Previsto no art. 5º, inciso VIII; art. 23, inciso III; art. 41 (atribuições)

03 INVENTÁRIO DE DADOS

Atendimento ao art. 37

04 FORTALECIMENTO DA SEGURANÇA DA INFORMAÇÃO

art. 6º, incisos VII e VIII; art. 38; art. 44; arts. 46 a 49; dentre outros.

05 REVISÃO DE CONTRATOS E CONVÊNIOS

art. 7º, 11, 19, 26 e para definição clara de responsabilidades de cada parte em relação à LGPD.

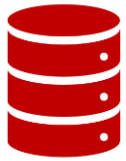
06 PROGRAMA DE CAPACITAÇÃO CONTINUADA

Para estimular uma cultura de privacidade desde a concepção, conforme art. 46 § 2º

01

Programa de Governança em +PRIVACIDADE

Governança em Privacidade



(i)

Governança de dados

1. Permitir que uma organização gerencie seus dados como um **ativo**;

2. Definir, aprovar, comunicar e implementar **princípios, políticas**, procedimentos, métricas, ferramentas e responsabilidades para **gerenciamento de dados**; e

3. Monitorar e orientar **atividades em conformidade** com políticas, uso de dados e gerenciamento

(ii)

Governança em privacidade

Exigida pelo §2º do **art. 50** da LGPD como **boa prática** para aplicação dos **princípios de segurança e prevenção** (princípios dos incisos VII e VIII do caput do art. 6º)

Voltada **somente para os dados pessoais**, que afetam diretamente o direito à privacidade das pessoas, ou seja, os dados pessoais conforme definido pela LGPD.

Programa de Governança em Privacidade

art. 50, inciso I LGPD

A Demonstrar **comprometimento** do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais

B Deve ser aplicável a **todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta

C Deve ser **adaptado** à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados

D Estabelecer **políticas e salvaguardas adequadas** com base em processo de **avaliação** sistemática de impactos e **riscos** à privacidade

E Ter o objetivo de estabelecer **relação de confiança com o titular**, por meio de atuação **transparente** e que assegure mecanismos de participação do titular

F Estar **integrado** a sua estrutura geral de **governança** e estabeleça e aplique mecanismos de supervisão internos e externos

G Contar com **planos de resposta a incidentes** e remediação

H Ser **atualizado** constantemente com base em informações obtidas a partir de **monitoramento contínuo e avaliações periódicas**

Inciso II Demonstrar a **efetividade** de seu programa quando apropriado e, em especial, **a pedido da ANPD** ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta

Comitê de Privacidade e Proteção de Dados Pessoais

TCESP Tribunal de Contas do Estado de São Paulo

O que é?

Boa prática no contexto da Governança em Privacidade

Facilitador da promoção de uma **cultura de proteção aos dados pessoais** dentro da instituição, ao mesmo tempo em que contribui para a tomada de decisão de forma centralizada, com a minimização, inclusive, de eventuais conflitos de interesse que possam existir

Núcleo para tomada de decisão em relação às ações que tratam de privacidade e proteção de dados, à luz da LGPD

Atribuições

(i) Propor **políticas e procedimentos** para adequação à LGPD;
(ii) Porta-voz da necessidade de seu **cumprimento e conscientização** de todos os agentes internos envolvidos com tratamento de dados pessoais;
(iii) **Gerenciar** atividades relativas ao tratamento de dados;
(iv) **Fiscalizar** processos que envolvem tratamento de dados pessoais;
(v) **Endereçar** problemas envolvendo produtos e serviços, no que se refere ao tratamento de dados;
(vi) **Acompanhar** legislações e orientações sobre o tema;
(vii) **Conduzir** análises e investigações;
(viii) Realizar o **inventário e o mapeamento de dados** e **relatórios de impacto à proteção de dados (RIPD)**

Fases da implantação do Programa de Governança em Privacidade

TCESP Tribunal de Contas do Estado de São Paulo

(i) Iniciação e Planejamento

- Conhecer o **cenário atual**
- Mapeamento geral das **informações e dados** importantes
- **Inventário** de dados pessoais
- Identificação de **contratos** que envolvem dados pessoais
- Alinhamento das **expectativas** com a alta administração

(ii) Construção e execução

Definir **parâmetros, regras e boas práticas**:

- Políticas e práticas para proteção da privacidade
- Cultura de segurança e proteção de dados e ***Privacy by Design***
- Relatório de Impacto à Proteção de Dados Pessoais (**RIPD**)
- Política de Privacidade e Política de Segurança da Informação
- Adequação de cláusulas contratuais
- Termo de Uso

(iii) Monitoramento

- Monitoramento de indicadores
- Registro constante e completo dos incidentes de segurança
- Processo de gestão de incidentes
- Análise e reporte de resultados
- Avaliação de melhorias – PDCA

TCESP
Tribunal de Contas
do Estado de São Paulo

02

O Encarregado de Dados

O encarregado pelo tratamento de dados pessoais

Artigo 41

O controlador de dados deverá **indicar um encarregado** pelo tratamento de dados pessoais.

O encarregado é o indivíduo responsável por **garantir a conformidade** de uma organização, pública ou privada, à LGPD.

§ 1º do artigo 41 da LGPD, **a identidade e informações de contato do encarregado** devem ser publicadas no sítio eletrônico do controlador

Obrigatoriedade

Entidades do Setor Público **devem** indicar um encarregado pelo tratamento de dados pessoais, como definido no art. 23, inciso III, da LGPD.

Atribuições do encarregado

§ 2º do art. 41

TCESP Tribunal de Contas do Estado de São Paulo

(i)

aceitar **reclamações e comunicações dos titulares**, prestar esclarecimentos e adotar providências;

- **Interagir com os titulares**, prestando esclarecimentos e adotando providências necessárias em razão desses contatos ou reclamações dos titulares

(ii)

receber **comunicações da autoridade nacional** e adotar providências;

- **Interagir com a ANPD**, sendo o ponto de contato para recebimento das comunicações da Autoridade, e responsável por adotar as providências requeridas
- **Cooperar com a ANPD**, sempre que demandado

(iii)

orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

- **Orientar os colaboradores** da entidade a respeito das práticas relacionadas à proteção de dados pessoais
- **Assessorar os responsáveis** pelo tratamento de dados pessoais na emissão do RIPD
- **Recomendar a realização de RIPD**, ou não, inclusive a metodologia de sua realização
- **Recomendar as salvaguardas** para mitigar riscos aos direitos dos titulares

(iv)

executar as **demais atribuições** determinadas pelo controlador ou estabelecidas em normas complementares.

- **Executar todas as atribuições** determinadas em normas complementares, da ANPD ou outros órgãos
- **Monitorar a conformidade** das atividades de tratamento de dados pessoais com a regulamentação e as normas vigentes
- **Decidir sobre a adequação** dos RIPD, e se as conclusões estão de acordo com a regulamentação, ou não

Perfil do encarregado

Quem pode ser?

Funcionário da instituição ou
agente externo, de natureza física ou jurídica.

Atenção

Evitar o conflito de interesses das atribuições do encarregado com outras funções que ele eventualmente exerça na instituição.

Como?

indicado por um ato formal, como um contrato de prestação de serviços ou um ato administrativo.

Requisitos funcionais

- Liberdade, independência e autonomia na realização de suas atribuições
- Acesso direto à Alta Administração da instituição.
- Bom nível de conhecimento das matérias envolvidas: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público
- Recursos humanos, tempo, orçamentários e infraestrutura adequados para realizar suas atividades

TCESP
Tribunal de Contas
do Estado de São Paulo

03

Inventário de dados

Inventário de Dados

O que é?

- **Diagnóstico** da situação atual
- Documento que registra **como é feito o tratamento de dados pessoais pela instituição**, verificando seu alinhamento ao previsto pelo art. 37 da LGPD
- Deve refletir o **caminho percorrido pelo dado pessoal** dentro da instituição, incluindo os processos e procedimentos pelos quais o dado transita
- Panorama geral dos dados pessoais sob posse da instituição
- Serve de subsídio para elaboração do Relatório de Impacto à Proteção de Dados Pessoais - RIPD

Deve ser registrado, para cada dado pessoal:

(i) **Fundamento** para sua coleta, a base legal usada para realizar o tratamento do dado pessoal

(ii) **Forma de coleta**, se diretamente do titular ou por outras fontes, incluindo coleta não digital

(iii) **Finalidade** do tratamento do dado pessoal, de acordo com a LGPD

(iv) **Medidas técnicas de segurança** para proteção do dado pessoal

(v) Se há **compartilhamento** desse dado, que departamentos internos ou outras instituições fazem o tratamento desse dados pessoais

(vi) O **descarte** do dado, ou seja, quando se dá o término do tratamento desse dado pessoal dentro da instituição.

TCESP
Tribunal de Contas
do Estado de São Paulo

04

Fortalecimento da Segurança da Informação

“Art. 46. Os agentes de tratamento devem adotar **medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§1º A autoridade nacional poderá dispor sobre **padrões técnicos mínimos** para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de **concepção do produto ou do serviço até a sua execução**.”

Medidas Técnicas e administrativas para proteger os dados pessoais - *Privacy by design*

§ 2º do art. 46: As medidas de que trata o caput deste artigo deverão ser observadas desde a **fase de concepção do produto ou do serviço até a sua execução**.

(i)

Proativo, e não reativo; preventivo, e não corretivo

Tomar medidas proativas e não reativas, **antecipando e prevendo eventos** que coloquem a privacidade em risco, antes que aconteçam

(ii)

Privacidade por padrão

Primar por entregar o **máximo grau de privacidade** e garantir que os dados pessoais são automaticamente protegidos em qualquer sistema de TI ou práticas de negócio

(iii)

Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada no projeto e arquitetura de sistemas de TI e práticas de negócio desde o projeto e **não se tratada como um apêndice**, a ser tratado em fases posteriores

(iv)

Funcionalidade total

Acomodar todos os interesses e objetivos legítimos, privilegiando o **ganha-ganha**, evitando falsas dicotomias como a privacidade versus a segurança ou privacidade versus usabilidade

Medidas Técnicas e administrativas para proteger os dados pessoais - *Privacy by design*

§ 2º do art. 46: As medidas de que trata o caput deste artigo deverão ser observadas desde a **fase de concepção do produto ou do serviço até a sua execução**.

(v)

Segurança ponta a ponta — proteção do ciclo de vida dos dados

A privacidade seja incorporada antes da coleta do primeiro dado e desdobrando-se por **todo o ciclo de vida dos dados** envolvidos, com medidas de segurança adequadas e fortes

(vi)

Visibilidade e transparência

Garantir que o tratamento de dados está de acordo com a **finalidade e objetivos** declarados, independentemente da prática comercial ou tecnologia empregada, e sujeito a verificação. É o tripé **Prestação de Contas (*Accountability*), Transparência (*Openness*) e Conformidade (*Compliance*)**;

(vii)

Respeito pela privacidade do usuário

Colocar o **interesse dos titulares em primeiro lugar**, oferecendo medidas e padrões rígidos de privacidade e facilidade de uso e interação

E quanto aos padrões técnicos mínimos?

“§ 1º A autoridade nacional poderá dispor sobre **padrões técnicos mínimos** para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.”

Regra de Pareto

TCESP Tribunal de Contas do Estado de São Paulo

3 ações que podem resolver 80% dos incidentes

Manter softwares Atualizados

"as 10 vulnerabilidades mais exploradas para o comprometimento de sistemas e redes governamentais são conhecidas e possuem correções, algumas há mais de 5 anos."

Hardening de SO e dispositivos

"especialmente para mudar configurações de fábrica alterando, por exemplo, usuário e senhas amplamente conhecidas e desabilitando protocolos inseguros ou não utilizados"

Melhorar processo de autenticação

"sistemas que utilizam apenas senhas como forma de autenticação são alvos mais fáceis para golpes digitais. Uma forma de melhorar a segurança dos sistemas é utilizar múltiplos fatores de autenticação"

Fonte: CETIC.br, detalhado em meu artigo:
Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques
https://bit.ly/2WcBanG

Boas práticas do mercado

Marco Civil da Internet
Decreto 8.771/16
Esse decreto define, por exemplo, a previsão de utilização de sistemas de **autenticação de dois fatores** e uso de **criptografia**.

Normas ABNT ISO/IEC

27001
Define os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um **Sistema de Gestão da Segurança da Informação** (SGSI), com foco nas necessidades e particularidades de cada organização

27002
Estipula as **melhores práticas** para apoiar a implantação do SGSI, incluindo a seleção, implementação e o gerenciamento de **controles**, com base em **análise de risco** da organização

27003
Diretrizes para **implantação do SGSI**

27004
Métricas e controles alinhados à 27002

27005
Trata do processo de **gestão de riscos** de segurança da informação

27006
Diretrizes para o **credenciamento de organizações e certificação de SGSI**

27035
Resposta e gerenciamento de **Incidentes**

27102
Diretrizes para **seguro cibernético**

27103
Uso do SGSI criar uma **estrutura de segurança cibernética**

27550
Diretrizes de engenharia de privacidade no **ciclo de vida de sistemas**

27701
Trata da **gestão da privacidade** no contexto da organização

31000
Traz recomendações para **gerenciar os riscos**

Padrões Técnicos de Segurança valorizados pelas autoridades europeias

TCESP Tribunal de Contas do Estado de São Paulo

1. Monitorar contas privilegiadas
2. Monitorar acesso e uso de BD com dados pessoais
3. Fazer o *hardening* de servidores
4. Usar criptografia em dados pessoais
5. Usar autenticação multifator
6. Ter rigoroso controle de acesso com base na necessidade
7. Realizar testes de invasão frequentes
8. Não armazenar senhas em texto claro
9. Registrar tentativas de login sem sucesso
10. Revisar códigos em busca de dados pessoais
11. Seguir padrão PCI DSS para processamento de dados de cartões

Fonte: Artigo: "Quais são os padrões técnicos mínimos exigidos pela LGPD?" https://bit.ly/3zIw1BA

TCESP
Tribunal de Contas
do Estado de São Paulo

05

Revisão de Contratos e Convênios

Revisão de Contratos

O que é?

- Análise de cada instrumento, inserindo cláusulas de observância à LGPD
  - Contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais
  - Instrumentos com eventuais operadores de tratamento de dados pessoais em nome do controlador
  - Contratos com funcionários, clientes e fornecedores

Exemplos:

(i) **Separação clara de responsabilidades** entre as partes do contrato, com a disposição de procedimentos de verificação e auditoria do cumprimento, incluindo, também, sanções e punições em caso do desrespeito à LGPD

(ii) Inclusão de **regras que definam padrões mínimos** de segurança da informação

(iii) Toda possibilidade de **transferência de dados** deve estar prevista e protegida por cláusulas específicas, além de ser preciso verificar se é **necessário o consentimento expresso** do titular e se tal transferência está alinhada com a atividade principal das partes

(iv) as partes devem concordar em **manter o nível de proteção** de dados alinhado no momento da assinatura do contrato, evitando que as ações de conformidade só sejam tomadas no início do ajuste

TCESP
Tribunal de Contas
do Estado de São Paulo

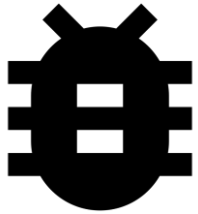
06

Programa de Capacitação Continuada

Causas dos incidentes

Ataques Maliciosos

52% no geral
47% no Brasil



Falhas de Sistemas

25% no geral
28% no Brasil

Erro Humano

23% no geral
25% no Brasil

Fonte: *Cost of a Data Breach Report* 2020, Ponemon Institute
https://bit.ly/39ErsOc

Principais vetores de *Ransomware*

E-mail *phishing*

E-mails falsos com o objetivo de roubar credenciais

Protocolo RDP

Protocolo Remote Desktop (RDP) é aquele que permite o acesso remoto a computadores por meio da Internet e que ficou muito comum em tempos de pandemia

Vulnerabilidades de softwares

Especialmente de sistemas operacionais, que permitem acesso ao computador da vítima para espalhar o *ransomware*.

Fonte: *o IC3[10] (Internet Crime Complaint Center), ligado ao FBI, em meu artigo "***Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

“

O **elo humano** é constantemente **negligenciado** em ações institucionais. Em relação à LGPD, é essencial que a instituição promova **treinamentos, capacitação, sensibilização e campanhas constantes** para servidores, contratados, jurisdicionados e parceiros que versem sobre **segurança da informação**, **privacidade** e cuidados necessários com o tratamento dos dados pessoais.

”

Referências

PONEMON INSTITUTE. Cost of a Data Breach Report 2020. Michigan: IBM Security, 2020. 82 p. Disponível em: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf. Acesso em: 01 jul. 2021.

VAINZOF, Rony. A LGPD e o Relatório de Impacto à Proteção de Dados Pessoais. 2021. Disponível em: https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. O encarregado de dados no setor público. 2021. Disponível em: https://www.migalhas.com.br/depeso/339636/o-encarregado-de-dados-no-setor-publico. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. Agentes de tratamento de pequeno porte: Conheça as propostas de flexibilização da LGPD para micro e pequenas empresas. 2021. Disponível em: https://www.migalhas.com.br/depeso/351410/propostas-de-flexibilizacao-da-lgpd-para-micro-e-pequenas-empresas. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. Quais são os padrões técnicos mínimos exigidos pela LGPD? 2021. Disponível em: https://mittechreview.com.br/quais-sao-os-padroes-tecnicos-minimos-exigidos-pela-lgpd/. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. Ransomware: pagar ou não pagar, eis a questão. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/ransomware-pagar-ou-nao-pagar-eis-a-questao-18052021. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. A experiência das autoridades europeias de proteção de dados como um modelo para a ANPD. 2021. Disponível em: https://mittechreview.com.br/a-experiencia-das-autoridades-europeias-de-protecao-de-dados-como-um-modelo-para-a-anpd/. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. Quais são os padrões técnicos mínimos exigidos pela LGPD?. 2021. Disponível em: https://mittechreview.com.br/quais-sao-os-padroes-tecnicos-minimos-exigidos-pela-lgpd/. Acesso em: 01 jul. 2021.

XAVIER, Fabio Correa. Qual o custo de incidente de violação de dados pessoais?. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/qual-o-custo-de-um-incidente-de-violacao-de-dados-pessoais-11072021. Acesso em: 01 jul. 2021

TCESP
Tribunal de Contas
do Estado de São Paulo

Obrigado!

"That's all Folks!"

Fabio Correa Xavier

Diretor do Departamento de TI do TCESP

https://www.linkedin.com/in/fabiocorreaxavier/

https://twitter.com/fabiocx